UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Criminal No. 13-107(DSD/FLN)

United States of America,

Plaintiff,

v. **ORDER**

Michael Duane Hoffman,

This matter is before the court upon the objection by defendant Michael Duane Hoffman to the June 27, 2013, report and recommendation of United States Magistrate Judge Franklin L. Noel. Based on a review of the file, record and proceedings herein, and for the following reasons, the court overrules the objection.

BACKGROUND

The background of this matter is fully set out in the report and recommendation, and the court summarizes only those facts necessary to resolve the current objection. In November and December 2012, the Internet Crimes Against Children Task Force conducted an investigation using a computer program called Ephex. Tr. 28:24-25. In that investigation, Minneapolis Police Officer Dale Hanson used Ephex to scan several peer-to-peer file-sharing networks. Id. at 29:1-13. Ephex identifies suspected child pornography files and logs the IP addresses sharing those files. Id. at 32:11-14.

On November 16, 2012, Ephex identified IP address 24.179.159.158 as sharing files suspected to include child pornography. Id. at 23:5-14. Hanson downloaded a number of files from the IP address, which were shared through the Shareaza file-sharing program. Id. at 24:2-6. An administrative subpoena later identified the IP address as belonging to Hoffman. Id. at 27:18-21. On the basis of these downloads, Hanson obtained a warrant to search Hoffman's residence. Id. at 27:22-24. Hoffman moves to suppress evidence obtained and statements made during the execution of the search warrant.

DISCUSSION

The court reviews the report and recommendation of the magistrate judge de novo. 28 U.S.C. § 636(b)(1)(C); Fed. R. Crim. P. 59(b); D. Minn. LR 72.2(b). Hoffman argues that the downloading of files from Shareaza constituted a warrantless search.

"When moving to suppress evidence on the basis of an alleged unreasonable search, the defendant has the burden of showing a legitimate expectation of privacy in the area searched." United States v. James, 534 F.3d 868, 872 (8th Cir. 2008) (citation and internal quotation marks omitted). "Whether a defendant has a constitutionally protected expectation of privacy involves a two-part inquiry - the defendant must show that (1) he has a reasonable expectation of privacy in the areas searched or the items seized,

and (2) society is prepared to accept the expectation of privacy as objectively reasonable." Id. at 872-73 (citation and internal quotation marks omitted).

In the present case, the magistrate judge correctly determined that Hoffman did not have a reasonable expectation of privacy in the searched computer files. Indeed, a defendant does not have a reasonable expectation of privacy in computer files "where [he] admittedly installed and used [a file-sharing program] to make his files accessible to others for file sharing." United States v. Stults, 575 F.3d 834, 842 (8th Cir. 2009). Hoffman argues that, unlike in Stults, there is no evidence that he installed the file-sharing program on his computer.

Stults, however, cannot be read to impose a requirement that Hoffman himself installed the file-sharing program. In fact, language elsewhere in Stults omits any mention of such a requirement. See id. ("Several federal courts have rejected the argument that an individual has a reasonable expectation of privacy in his or her personal computer when file-sharing software ... is installed."). Moreover, post-Stults courts do not require a showing that the defendant installed the file-sharing program. See, e.g., United States v. Hill, No. 10-05044-01-CR-SW-RED, 2012 WL 2735329, at *2 (W.D. Mo. June 18, 2012), adopted by 2012 WL

2734039 (July 9, 2012) ("There is no reasonable expectation of privacy in computer files that are accessible to users of a computer network." (citation and internal quotation marks omitted).

In his interview with law enforcement, Hoffman indicated that he was the main user of the computer and was aware that he had shared files through Shareaza. The knowing use of a file-sharing program defeats any claim of a reasonable expectation of privacy in the files shared on that network. Cf. Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citations omitted)). As a result, no search in violation of the Fourth Amendment occurred.[1] Therefore, after a de novo review, the court overrules the objection.

CONCLUSION

Accordingly, **IT IS HEREBY ORDERED** that:

1. Defendant's objection to the report and recommendation [ECF No. 36] is overruled;

[1] Hoffman also argues that even if his awareness of file-sharing is sufficient to defeat an expectation of privacy, law enforcement agents did not have information regarding his awareness and use at the time of the alleged search. This argument is unavailing. The sequence of investigation in the instant matter is materially indistinguishable from that in Stults. See Stults, 575 F.3d at 838-39 (noting that law enforcement officers downloaded files from anonymous IP address, filed administrative subpoena and obtained a search warrant before interviewing defendant, who admitted to installing and using file-sharing program).

2. The report and recommendation [ECF No. 34] is adopted in its entirety; and

3. The motions to suppress [ECF Nos. 21, 22] are denied.

Dated: August 1, 2013

s/David S. Doty
David S. Doty, Judge
United States District Court